WHITE PAPER

Governance, Risk, and Compliance use case guide

servicenow

Table of contents

Integrated Risk Program

Imagine having the ability to manage risk—be it digital, IT, compliance, or vendor—across every department and function, without slowing down processes and over-burdening your team. Picture a scenario where previously siloed processes become part of an integrated risk program that extends across the enterprise. With ServiceNow, you can make this vision a reality.

Everyone knows the risks that come with regulatory non-compliance and ignoring vulnerabilities. But the threats continue, and they're constantly evolving. Inefficient processes, human error, new initiatives like digital transformation, and unforeseen delays all increase risk. The reality is that, despite the best intentions, critical items keep falling through the cracks—and most companies can't even identify what fell through, let alone the potential impact if left unchecked.

At the same time, complexity keeps growing with each new regulation, process, application, and piece of hardware. It's no surprise that legacy governance, risk, and compliance (GRC) products can't keep up with this growing list of challenges.

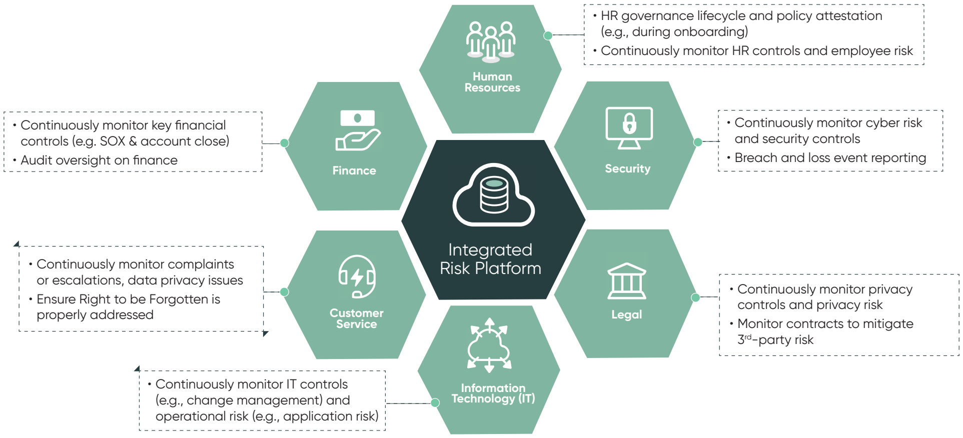
To manage risk and compliance in this ever changing landscape you need a modern, cloud-based platform that can continuously monitor activities, improve decision making, and increase performance through automation and AI powered user experiences. You can work the way you want with support to easily collaborate with other departments and effectively communicate with business users, the CEO, and the board. And user-friendly portals with mobile interfaces make it easy to work anytime and anywhere.

Designed for cloud scale, the Now Platform® consolidates data from across the enterprise and from third parties using open APIs so you can share data and automate cross-functional workflows. Processes seamlessly embed risk and compliance activities, collect evidence, assign tasks, and streamline audits. Built on the Now Platform, ServiceNow GRC identifies business risks through continuous monitoring and risk events, which then roll up to the enterprise. And we reduce compliance complexity with a common control framework, so you can "test once and comply many"—which also delivers significant efficiency gains. It's time to change the way work gets done with ServiceNow.

With risk and compliance embedded in cross-functional workflows you can easily and confidently manage risk across the enterprise. An HR compliance violation could trigger a legal issue. The risk posed by a vendor with degrading security performance could lead you to restrict their access to your network. You can handle risk with confidence. Take the right action—and take it sooner—so your business stays protected.

Let's take a closer look at some common risk and compliance management challenges:

1. Monitor for critical vulnerabilities and understand the business impact
2. Identify and address misconfigurations before they become business risks
3. Ensure your compliance program effectively supports your business services
4. Monitor HR policy requirements and identify on-boarding risk
5. Ensure privacy standards are met



- HR governance lifecycle and policy attestation (e.g., during onboarding)
- Continuously monitor HR controls and employee risk

- Continuously monitor key financial controls (e.g. SOX & account close)
- Audit oversight on finance

- Continuously monitor cyber risk and security controls
- Breach and loss event reporting

- Continuously monitor complaints or escalations, data privacy issues
- Ensure Right to be Forgotten is properly addressed

- Continuously monitor privacy controls and privacy risk
- Monitor contracts to mitigate 3rd-party risk

- Continuously monitor IT controls (e.g., change management) and operational risk (e.g., application risk)

> 68% of organizations have had significant business disruption due to a risk event.
>
> – NC State PCM

> 82% of organizations are going through a digital transformation.
>
> – Gartner 2019

> 216 average daily alerts show the increasing rate of regulatory change.
>
> – Reuters 2018

> 57% of victims were breached due to a vulnerability for which a patch was available.
>
> – Ponemon

References

1. State of Risk Oversight, NC State PCM, Enterprise Risk Management Initiative, Spring 2019
2. Gartner CEO Survey April 2019
3. Thomson Reuters: Cost of compliance 2018
4. Ponemon state of vulnerability response – patchwork demands attention

Use case: Monitor for critical vulnerabilities and understand the business impact

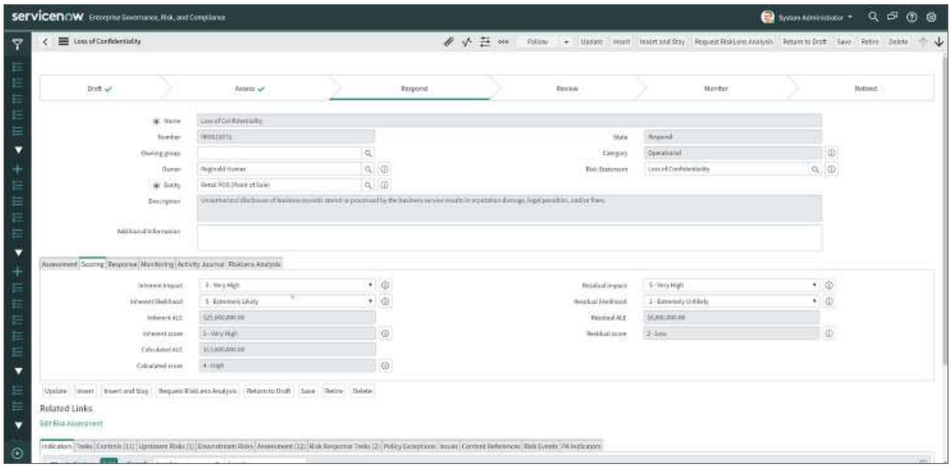
With legacy solutions, it's an ongoing challenge to manage security vulnerabilities and risk across multiple departments and functions. Someone on the security team may be able to spot a vulnerability due to a missing application patch—but it takes an integrated risk platform to tell you that the vulnerability affects the point of sale system with the potential for millions in lost revenue. An integrated risk management program can help you gauge the associated risk in relation to all others and track it through to resolution. You can also easily communicate the risk status and potential business impact to upper management.

Imagine a security manager tracking 50 identified vulnerabilities. That person might not notice that one patch isn't installed correctly. Maybe a machine is offline when the patches push out, or the patch depends on other updates to fully address the vulnerability. Whatever the reason, vulnerabilities like these linger unless you have an integrated risk program to identify and enforce the needed security.

Working through ServiceNow Vulnerability Response, ServiceNow GRC collects data from a variety of vulnerability scanners. It can then identify outstanding vulnerabilities and prioritize each based on severity, the availability of exploits, relative risk (based on a customizable score), and the potential impact on services (based on asset and business insights). Issues get automatically routed to the correct vulnerability manager for immediate resolution, and a prescribed path to remediation of a given vulnerability can be selected within Vulnerability Solutions Management. Dashboards provide real-time updates to the risk manager and business stakeholders. And decision makers can easily quantify and manage the overall risk posture of the enterprise.

A risk manager at work:

As a risk manager, I have the responsibility to monitor threats on a minute-by-minute basis. I can see on my ServiceNow Risk dashboard that a new critical risk has appeared. Drilling into the alert reveals that the point of sale (POS) system has an unpatched vulnerability and reveals insights into the exploitability of this item. The issue can affect overall system availability and make us vulnerable to fraud or data theft. Without ServiceNow, I would waste time figuring out who should address the issue. Instead, I can immediately see the correct people on the security and IT teams responsible for taking action. The ServiceNow GRC risk management application also automatically calculates the risk score considering the threat and the potential loss if we leave it unaddressed.



Name	Loss of Confidentiality
Number	[illegible]
Owning group	
Owner	Reginald Humes
Entity	Retail POS (Point of Sale)
Description	Unauthorized disclosure of business records stored or processed by the business service results in reputation damage, legal penalties, and/or fines.
Additional information	
State	Respond
Category	Operational
Risk Statement	Loss of Confidentiality
Inherent impact	5 - Very High
Inherent likelihood	5 - Extremely Likely
Inherent ALE	$25,000,000.00
Inherent score	5 - Very High
Calculated ALE	$13,000,000.00
Calculated score	4 - High
Residual impact	5 - Very High
Residual likelihood	1 - Extremely Unlikely
Residual ALE	$5,000,000.00
Residual score	2 - Low

Figure 1: Risk is calculated based on business impact.

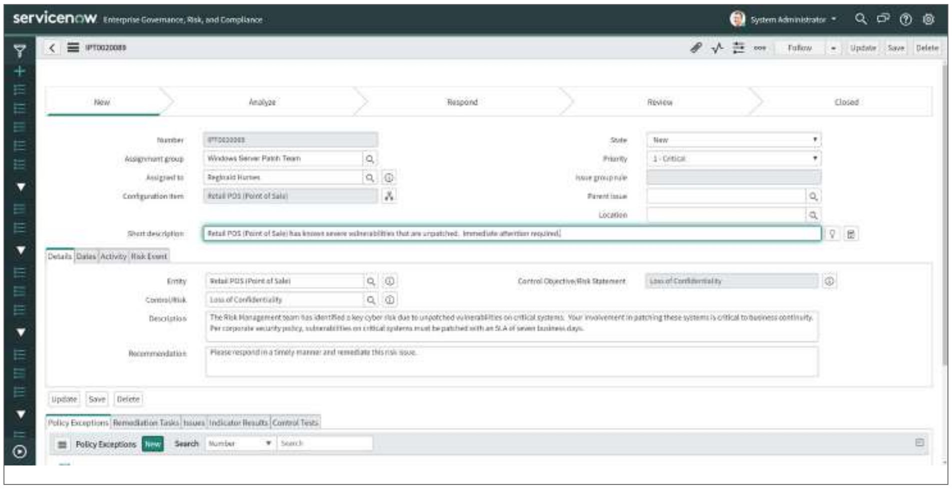
For this particular threat, the risk score is high and the calculated average loss expectancy (ALE) is almost $14M. If the calculations were within our predefined risk threshold of $8M, I could accept it. In this case, the level of risk is unacceptable and I need to take action.

I can see this vulnerability has been active for two weeks. By clicking on the indicators related list, I can also identify which device has the unpatched vulnerability. A combination of continuous risk monitoring capabilities for essential business services and out-of-the-box risk indicators from ServiceNow helped us spot the risk.

Looking at my controls list, I can see that "Manage change requests," "Manage changes," and "Establish and maintain a patch management program" are missing. I can immediately add these controls from this form.

When the system first identified this risk, it automatically created an issue and sent it to the appropriate team.

I can drill down into the issue created from the issues list. I know some organizations might engage the vulnerability manager at this point, but because this was a Windows machine, we have a special Windows patch team I want to alert. From within the issue, I can track progress and, if necessary, work with other parts of the organization to resolve the issue quickly without endless exchanges of email.



Number: IPT0020089
Assignment group: Windows Server Patch Team
Assigned to: Reginald Humes
Configuration item: Retail POS (Point of Sale)
State: New
Priority: 1 - Critical
Issue group rule:
Parent issue:
Location:
Short description: Retail POS (Point of Sale) has known severe vulnerabilities that are unpatched. Immediate attention required.
Entity: Retail POS (Point of Sale)
Control/Risk: Loss of Confidentiality
Control Objective/Risk Statement: Loss of Confidentiality
Description: The Risk Management team has identified a key cyber risk due to unpatched vulnerabilities on critical systems. Your involvement in patching these systems is critical to business continuity. Per corporate security policy, vulnerabilities on critical systems must be patched with an SLA of seven business days.
Recommendation: Please respond in a timely manner and remediate this risk issue.

Figure 2: The issue is automatically created with the appropriate priority and assigned to the owner of the affected asset.

When the Windows patch team has completed the patch, the security team can rescan our systems. If the vulnerability is resolved, the critical risk will disappear from my Risk Dashboard and the issue will close automatically. The system tracks all status updates within the issue—providing an audit trail for future reference.

With an integrated platform, all teams (security, risk, and IT) have access to the same underlying information, presented by dashboards designed specifically for each team. We can use this information to prioritize security vulnerabilities in relation to all other business risks for a holistic risk management program.

Tech Tip: Check out the new risk indicator templates within ServiceNow GRC. Go to Risk Management > Risk Statement > Risk Framework.

Use case: Identify and address misconfigurations before they become business risks

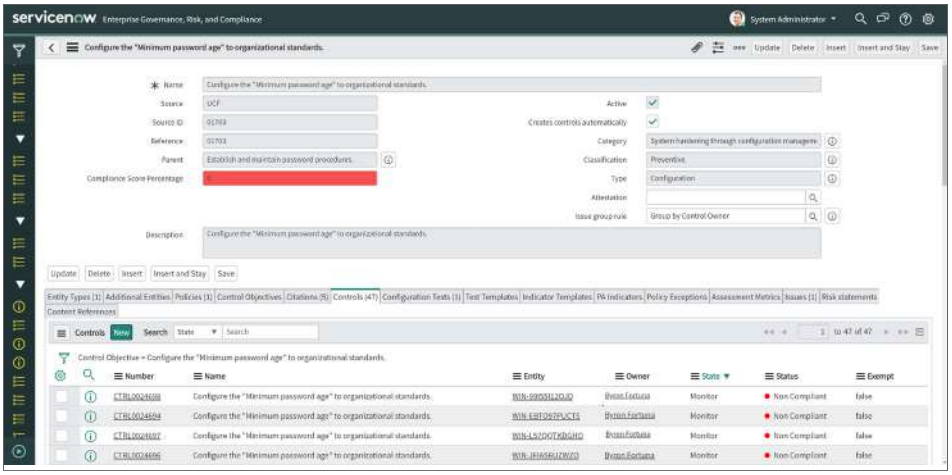
It's not unusual for IT teams to maintain thousands of different software packages, systems, and devices. While most teams have processes in place to verify configurations, mistakes still happen. A newly installed router may have a password entered in clear text which leaves it visible. Maybe an access control for a new firewall isn't set up properly, leaving an opening for intruders. Or the user of a device has admin privileges and can install unauthorized software or change important security settings, which could leave an opening for an attacker to gain unrestricted access to your network. Standards and external regulatory compliance obligations (for example SOX, PCI, and ISO) often include elements that attempt to address the business risk of misconfigured software, older protocols, and weak passwords. Enterprises translate these requirements into configuration hardening policies.

Too often, organizations only identify misconfigurations after an attack. A better approach is to identify the misconfigurations before they put your business at risk.

Working through ServiceNow Security Operations Configuration Compliance, you can monitor data from security configuration assessment tools. But you want to extend continuous monitoring with ServiceNow GRC to the configuration hardening policies so you can identify a failed configuration test result, assess the potential business impact, automatically create an issue, and proactively engage the responsible party to address the weakness before it is exploited.

A compliance manager at work

Several failed controls have popped up on my Policy and Compliance dashboard. Drilling into them, I see that the latest scan by our security configuration assessment tool has spotted misconfigured software. The data shows multiple windows servers that don't have the appropriate setting for minimum software password age, meaning there may never be a prompt to change the password to access the hardware–which creates an opportunity for a clever attacker. This could be the result of a software update or new installation.



Configure the "Minimum password age" to organizational standards.

Name	Configure the "Minimum password age" to organizational standards.
Source	UCF
Source ID	01703
Reference	01703
Parent	Establish and maintain password procedures.
Compliance Score Percentage	0
Active	☑
Creates controls automatically	☑
Category	System hardening through configuration manageme
Classification	Preventive
Type	Configuration
Attestation	
Issue group rule	Group by Control Owner
Description	Configure the "Minimum password age" to organizational standards.

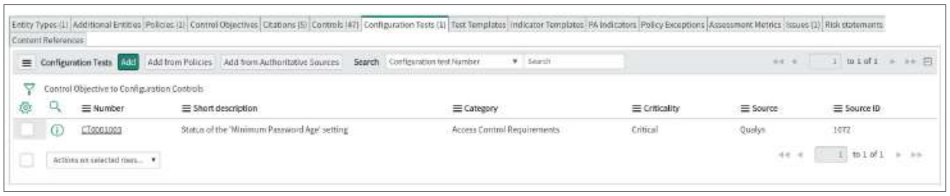
Controls — Search: State

Control Objective = Configure the "Minimum password age" to organizational standards.

Number	Name	Entity	Owner	State	Status	Exempt
CTRL0024698	Configure the "Minimum password age" to organizational standards.	WIN-99I55H12OJD	Byron Fortuna	Monitor	● Non Compliant	false
CTRL0024694	Configure the "Minimum password age" to organizational standards.	WIN-EBTO97PUCTS	Byron Fortuna	Monitor	● Non Compliant	false
CTRL0024697	Configure the "Minimum password age" to organizational standards.	WIN-L57OOTKBGHD	Byron Fortuna	Monitor	● Non Compliant	false
CTRL0024696	Configure the "Minimum password age" to organizational standards.	WIN-JFIA5RJZWZO	Byron Fortuna	Monitor	● Non Compliant	false

Figure 3: Continuous monitoring of controls show the entities affected and identify any policy exceptions.

To transfer the scan data used by GRC Continuous Monitoring into the Now Platform, an enterprise must integrate with ServiceNow Security Operations. Then, the scan data is imported into the Configuration Compliance application, where failed configuration test results are matched against assets in the ServiceNow Configuration



Entity Types (1) | Additional Entities | Policies (1) | Control Objectives | Citations (5) | Controls (47) | Configuration Tests (1) | Test Templates | Indicator Templates | PA Indicators | Policy Exceptions | Assessment Metrics | Issues (1) | Risk statements | Content References

Configuration Tests | Add | Add from Policies | Add from Authoritative Sources | Search: Configuration test Number ▼ | Search | 1 to 1 of 1

Control Objective to Configuration Controls

Number	Short description	Category	Criticality	Source	Source ID
CT0001003	Status of the 'Minimum Password Age' setting	Access Control Requirements	Critical	Qualys	1072

Actions on selected rows... ▼ | 1 to 1 of 1

Figure 4: The Configuration Tests tab shows the source used to collect configuration data.

Management Database (CMDB). Data from the CMDB determines how important each asset is to the business, and the resulting criticality assessment is one factor in the automated risk score calculation used to prioritize failed results.

Just as my Policy and Compliance dashboard displayed the failed controls, my GRC Risk dashboard displays the risks associated with these misconfigurations in relation to all other identified risks across the enterprise. And the IT manager can see the criticality level of the failed test results on the Configuration Compliance dashboard.

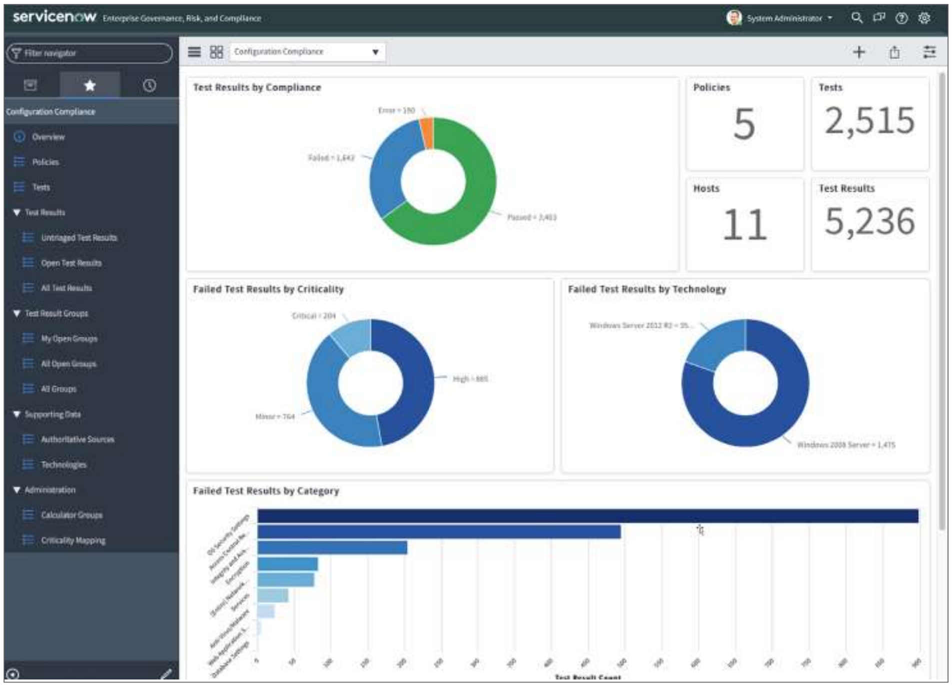


Figure 5: The Configuration Compliance dashboard is dynamically updated based on new test results.

Although I could have had each non-compliant control automatically generate an issue and send it to the IT manager, I would rather review configuration test failures before routing issues to the appropriate person. Because we're experiencing the same control failing across multiple assets, I've elected to group the issues under a single parent issue with a single remediation task before assigning the grouping to the IT manager.

If this type of issue becomes a common occurrence, I may create a rule to automatically group similar issues under a predefined parent issue to automate the process. I can then track the parent issue to completion.

IT will update the issue, so I will know whether the configuration change will happen during the next update cycle when the security team or IT will review and approve the change. Each team has visibility into the current status of the change, the next steps, and who is responsible.

When a subsequent scan shows the configuration issue has been remediated (in other words, there is no longer a configuration test failure), the control will again be compliant. When the IT manager closes the parent issue, providing proof that the remediation process was successful, all child issues will also close.

Tech Tip: When you identify several similar issues, use grouping to make tracking easier.

Use case: Ensure your compliance program effectively supports your business services

Behind the curtain that separates the front office from the back is a battalion of systems, processes, and hardware that supports every aspect of an enterprise. You'll also find a variety of tools monitoring those systems—tools that create a mountain of data pertaining to violations alone. Some basic violations include:

Incidents:

- Access, including creation, change, and termination (tasks include retrieving a laptop and badge and removing an employee from Active Directory)
- Unauthorized access to an asset holding data that's mission-critical to an organization or PII
- Security incidents
- Unpatched systems

Changes with in-scope systems:

- Changes to hardware or software without approval or a backout plan
- Emergency change compliance

The effort required to comb through the data manually to uncover and prioritize the most critical risks to the business is formidable. Without automated processes to ensure compliance, the owners of the systems, processes, and hardware fall back on a manual process to attest that they follow the proper policies.

Anytime there is manual work to manage mountain of data there is a high risk that issues might slip through the cracks and errors will be made. Using a single, integrated platform you can be confident that the most critical issues are identified and recapture thousands of work hours for more engaging projects.

And with ServiceNow, you can use the same integrated risk platform you rely on every day to easily and confidently prove compliance and provide supporting evidence for audits. When you know you have the right controls in place and can efficiently and effectively prove compliance, audits become virtually painless.

An audit manager at work:

As an internal auditor, I know from experience that planning is important. Recently, I've been working on my audit plan for the year. The business control owners have completed the risk assessments I sent them, and I've defined the scope of my audit for this year to include the following:

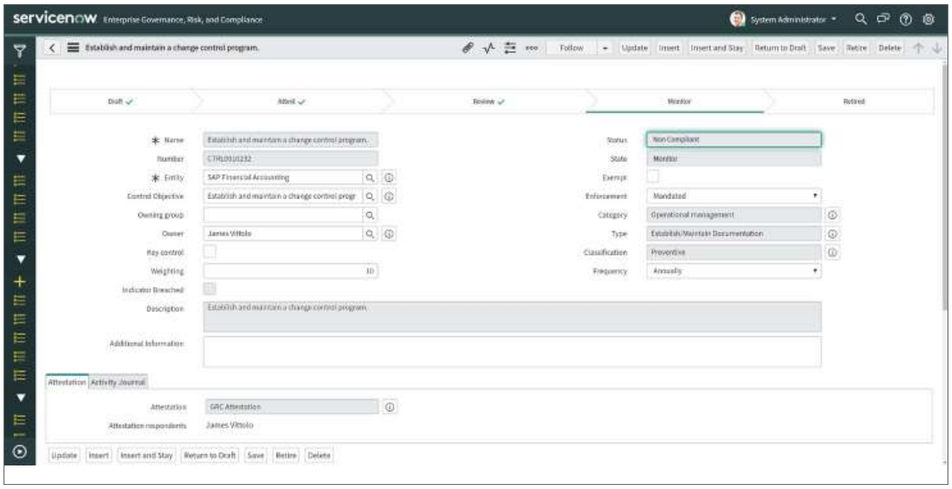
- PCI environment
- SOX environment
- SAP Financial Accounting business service
- Linux servers
- Server hardening

These were all defined in my Configuration Management Database (CMDB), so scoping them was easy. I don't have a very mature CMDB, but I have made sure the 20 most critical assets, processes, and systems are represented correctly.

Based on the results of my risk assessments, I've decided to begin my audit with the SAP Financial Accounting business service.

I can see from my dashboard that I have a compliance violation. Specifically, the proper change management processes haven't been followed.

When I investigate the changes being monitored, it appears someone implemented a change without a backout plan. The system automatically created an issue for the SAP Financial Accounting service owner.



Establish and maintain a change control program.

* Name	Establish and maintain a change control program.	Status	Non Compliant
Number	CTRL0010232	State	Monitor
* Entity	SAP Financial Accounting	Exempt	□
Control Objective	Establish and maintain a change control progr	Enforcement	Mandated
Owning group		Category	Operational management
Owner	James Vittolo	Type	Establish/Maintain Documentation
Key control	□	Classification	Preventive
Weighting	10	Frequency	Annually
Indicator Breached	□		
Description	Establish and maintain a change control program.		
Additional Information			

Attestation	GRC Attestation
Attestation respondents	James Vittolo

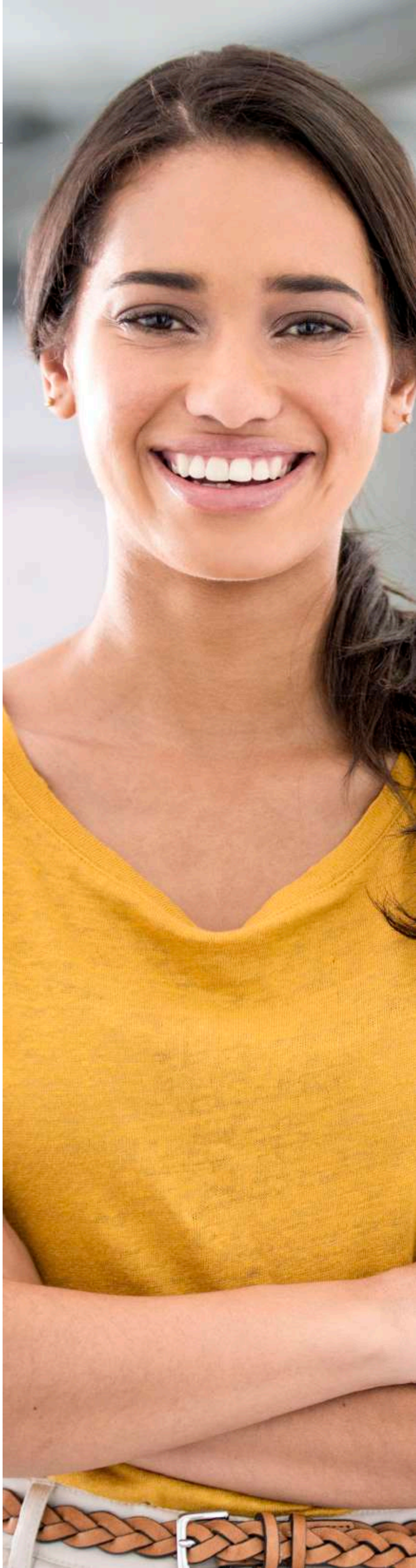
Figure 6: Regular monitoring ensures best practices are being followed.

The service owner decides to delegate the issue to a teammate using the Assignment group field. The teammate's job is to investigate why this is happening and answer questions such as: Is there a training opportunity? Do we have a history with this type of issue?

There is a discussion with the manager of the team members causing the violations. The history of the issue goes back just a few weeks because the team members are new. Since they recently joined the company there is a clear need for training. The team manager promises to send the new members an attestation with a link to the change management policy. The team members must read the policy and confirm that they understand it.

The issue is closed with a note stating that the "Manager will ensure proper training." I'm able to see that the issue is closed along with the notes from the investigation and we keep a close watch to ensure resolution.

When the external audit team arrives, they can check the current status of our controls. If they want, they can look at past results, the failures we spotted, our responses, and the complete audit trail of our actions. This data provides them with a significantly higher level of confidence and helps to streamline our audit process.



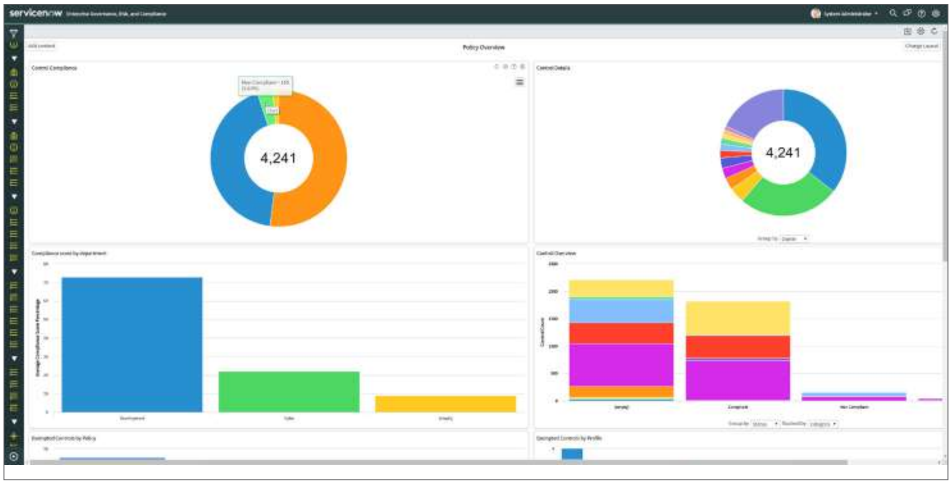

servicenow
Policy Overview
Control Compliance
4,241
Control Details
4,241
Compliance score by department
Control Overview
Exempted Controls by Policy
Exempted Controls by Profile

Figure 7: Interactive dashboards let you drill down into any report for greater detail.

Tech Tip: As a starting point for populating your CMDB, define a minimum desired state. For example, a common criterion is "A server exists in the CMDB only if it has a relationship to at least one application." Otherwise, it's difficult to tell what the server is used for. ServiceNow allows you create this type of requirement, so in the event of a violation, a notification would be automatically sent to the appropriate person in IT or a task would be created to define the application for the offending server.

You can also make use of data certification to maintain your CMDB with clean information. In ServiceNow, you can schedule tasks at a specified frequency for application owners to attest whether the application they are responsible for accesses Personally Identifiable information (PII), is Internet-facing, or accesses credit card data (protected by PCI). The responses are saved directly to the CMDB.

Use case: Monitor HR policy requirements and identify an on-boarding risk

HR teams frequently use multiple, standalone point solutions to support different aspects of HR. You might use one system for on-boarding and another to manage policies, but the policies don't always map back to appropriate controls. And there are a wide range of regulations across the employee journey. Beyond internal policies and best practices there are regulations that can vary greatly from state to state and country to country. When these systems run in silos, teams are left with manual work to try and monitor compliance across the organization.

- Is your company subject to local laws regarding pay for unused personal time off?
- Have all appropriate steps been followed during on-boarding and termination?
- When was the last time employees confirmed the review of anti-harassment and insider trading policies?
- Have the appropriate pre-employment background checks been completed?
- How do leave policies vary depending on where an employee resides?
- Have the appropriate policies been followed for whistleblowers, non-discrimination, sexual harassment complaints, and investigations?
- Have you implemented and approved the appropriate policies regarding separation of duty?

Fortunately, there's a relatively simple way to mitigate these risks. With a robust solution like ServiceNow HR Service Delivery working in tandem with ServiceNow GRC, you have an integrated risk platform and an additional line of defense. GRC can monitor activity across solutions, automatically alert the appropriate teams when there is a compliance concern, track the concern through resolution, and prove that your organization has adhered to all requirements.

The bottom line: our integrated risk platform lets you spend time on people, not processes.

An HR manager at work:

As the talent manager, I need to work with my team to ensure that our organization is following all the local regulations and our internal policies. These can vary greatly, depending on employee location. In my ServiceNow dashboard, I can view reports specifically configured to help me track our compliance efforts. In one case, I can see an on-boarding risk resulting from an HR task that was closed but never completed. The HR compliance manager is identified, as is the new employee.

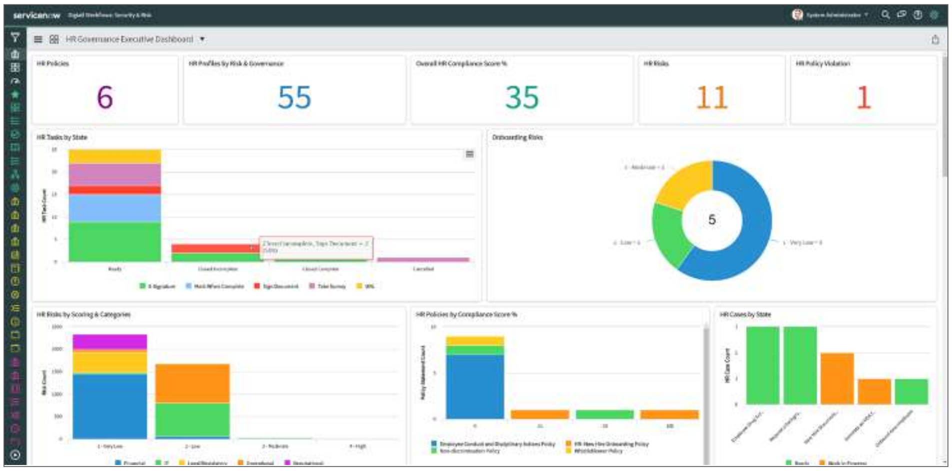
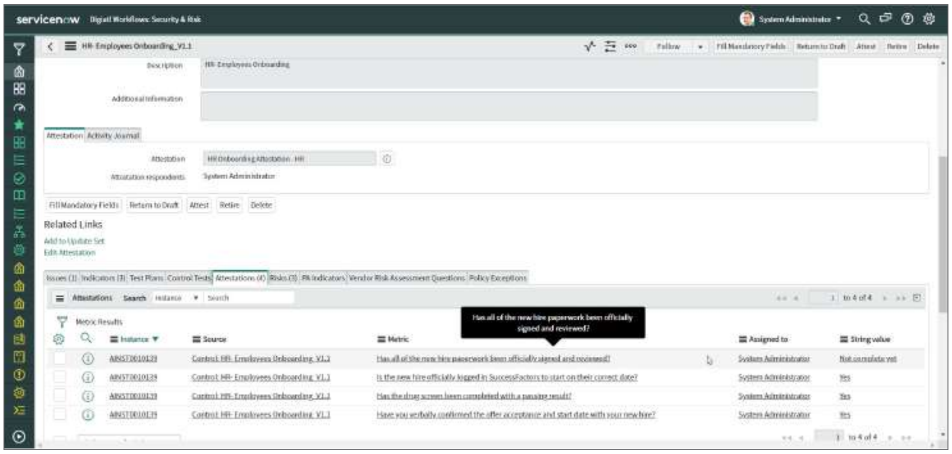


Figure 8: Drag and drop reports into your dashboard so it meets your unique needs.

When I drill into the closed but incomplete task, I see that a new employee (a much-needed account executive) hasn't signed a required NDA as part of the on-boarding process—but the hiring manager has signed off on the case. Looking at the risk, I can see it could have a significant impact on the business. The account executive is scheduled to start tomorrow. This is in direct violation of our process.

GRC automatically identified the risk, but I can also see that the HR compliance manager noticed the error. When I look at the compliance manager's attestations, I see they indicated that the new-hire paperwork was not complete.



Description: HR- Employees Onboarding

Additional information:

Attestation: HR Onboarding Attestation - HR

Attestation respondents: System Administrator

Instance	Source	Metric	Assigned to	String value
AINST0010139	Control: HR- Employees Onboarding_V1.1	Has all of the new hire paperwork been officially signed and reviewed?	System Administrator	Not complete yet
AINST0010139	Control: HR- Employees Onboarding_V1.1	Is the new hire officially logged in SuccessFactors to start on their correct date?	System Administrator	Yes
AINST0010139	Control: HR- Employees Onboarding_V1.1	Has the drug screen been completed with a passing result?	System Administrator	Yes
AINST0010139	Control: HR- Employees Onboarding_V1.1	Have you verbally confirmed the offer acceptance and start date with your new hire?	System Administrator	Yes

Figure 9: Attestations allow you to ensure policies are being followed.

When the system identified the risk, it automatically generated an issue and sent it to the HR compliance manager. That person will work with the hiring manager to resolve this before tomorrow. The new employee will see the NDA in their to-do list on the employee portal.

This situation also highlights the fact that we need to do more training for our hiring managers. I'll create a task for the HR compliance manager to schedule a meeting so we can discuss how this happened and modify our process, if necessary. The HR compliance manager should create a task for the hiring manager to repeat the online training for the hiring process. If I don't see it before our meeting, I'll have the compliance manager create it directly afterward.

I'm also going to monitor that the related issue and tasks are closed. When the signed document is uploaded, it will clear the violation on my dashboard.

We follow a similar process to ensure that new employees acknowledge anti-harassment, insider trading, and other policies during the on-boarding process. ServiceNow GRC continuously monitors for compliance across all policies and regulations and helps us build a consistent response process that includes an audit trail.

The CHRO can also have a real-time view of the organization's global risk posture through dynamic dashboards tailored to their needs. And the CHRO can easily share information with other executives and board members, making it simpler for the team to prove compliance.

Use case: Ensure privacy standards are met

The implementation of the General Data Protection Regulation (GDPR) has had an impact on virtually every company in the world with an online presence. Given the GDPR's hefty fines of up to 4% of global annual revenue, companies are taking precautions to ensure compliance. One added benefit is that, by complying, they are protecting their own reputation with customers.

However, GDPR isn't the only data privacy regulation that organizations must follow. Countries such as Japan, Australia, Brazil, Canada, and the United States are either drafting or have approved similar data privacy legislation—adding to the compliance burden.

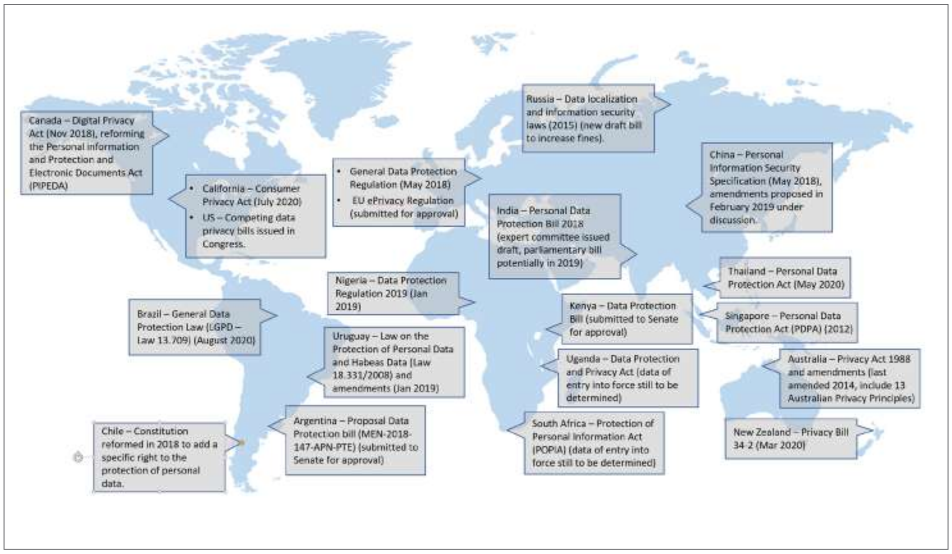

Canada – Digital Privacy Act (Nov 2018), reforming the Personal information and Protection and Electronic Documents Act (PIPEDA)
• California – Consumer Privacy Act (July 2020)
• US – Competing data privacy bills issued in Congress.
• General Data Protection Regulation (May 2018)
• EU ePrivacy Regulation (submitted for approval)
Russia – Data localization and information security laws (2015) (new draft bill to increase fines).
China – Personal Information Security Specification (May 2018), amendments proposed in February 2019 under discussion.
India – Personal Data Protection Bill 2018 (expert committee issued draft, parliamentary bill potentially in 2019)
Nigeria – Data Protection Regulation 2019 (Jan 2019)
Thailand – Personal Data Protection Act (May 2020)
Brazil – General Data Protection Law (LGPD – Law 13.709) (August 2020)
Kenya – Data Protection Bill (submitted to Senate for approval)
Singapore – Personal Data Protection Act (PDPA) (2012)
Uruguay – Law on the Protection of Personal Data and Habeas Data (Law 18.331/2008) and amendments (Jan 2019)
Uganda – Data Protection and Privacy Act (data of entry into force still to be determined)
Australia – Privacy Act 1988 and amendments (last amended 2014, include 13 Australian Privacy Principles)
Chile – Constitution reformed in 2018 to add a specific right to the protection of personal data.
Argentina – Proposal Data Protection bill (MEN-2018-147-APN-PTE) (submitted to Senate for approval)
South Africa – Protection of Personal Information Act (POPIA) (data of entry into force still to be determined)
New Zealand – Privacy Bill 34-2 (Mar 2020)

Figure 10: The number of privacy regulations are growing adding complexity for global organizations.

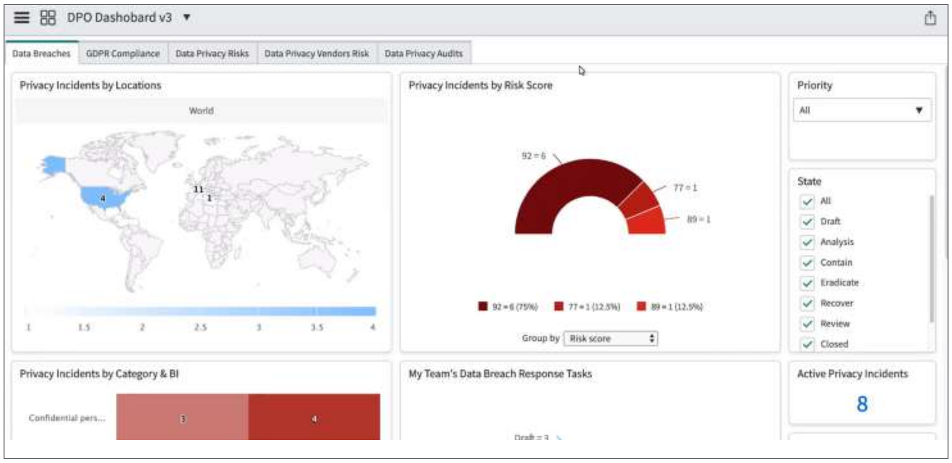
At ServiceNow, we take a different approach to compliance which allows you to easily meet all of the different privacy regulations. We identify the applications that touch personal data and gather supporting evidence while tracking application compliance across functional groups. Access to critical information regarding risks, controls, vendor information, and security data is streamlined. Rapidly identify threats, improve efficiency, and protect your customers sensitive data.

Key ServiceNow privacy protection capabilities include:

- Importing data privacy requirements and descriptions through Policy Management
- Distributing and tracking Data Protection Impact Assessments (DPIAs)
- Executing risk evaluations and managing issues
- Managing audit engagements
- Addressing data subject requirements and requests
- Facilitating Personally Identifiable Information (PII) mapping
- Addressing 72-hour breach notifications
- Managing third-party data privacy compliance
- Addressing Data Protection Officer (DPO) requirements and providing visibility

A Data Protection Officer (DPO) at work:

As the Data Protection Officer (DPO), I need to make sure the policy and risk posture of my organization is strong. To do that, I need real-time visibility into security privacy events, risks, and compliance violations that could affect the business. I've built my dashboard with those things in mind.



Priority: All ▼

State
☑ All
☑ Draft
☑ Analysis
☑ Contain
☑ Eradicate
☑ Recover
☑ Review
☑ Closed

Group by: Risk score

Active Privacy Incidents: 8

Figure 11: The Data Protection Officer needs real-time visibility into the security and risk posture of their organization.

One of my dashboard reports shows me data breaches by level of risk, and it indicates there is something I should be acting on. I have here 6 major incidents with high risks. By clicking on the report, I can see there are 4 major security incidents in the United States. Drilling into the incidents in New York I see that one of the incidents is linked to a possible attack on a server. Drilling in further I see that my team has already analyzed and tagged it as a privacy concern using the GDPR tag. As part of the workflow, the system automatically emails me and creates a task when the risk is escalated so that it appears on my dashboard.

When an incident is tagged as GDPR, the system automatically generates a new task for Security and IT, informing them of the new risk. I can now drill into more details to find out how this incident occurred and how to prevent it from happening again. I acknowledge that a breach occurred and once I close my task the system automatically alerts legal, PR, and other critical response teams. The workflow also updates and includes tasks to execute the data privacy response plan.

A link to the security incident is now part of the record and identifies which business service or entity is affected. In this case the incident impacts SAP Financial Accounting and involves a third party. I can select the vendor and see there is a risk that the vendor may have disclosed confidential information. The risk is calculated as moderate, which is higher than I'd like because my risk appetite is very low. I can also see the mitigating controls and some are non-compliant resulting in the moderate risk rating. The controls are common for the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

This incident causes the system to automatically trigger privacy and security assessments which are sent through the Vendor Risk Management vendor portal. I'll watch for these assessments to come back and keep an eye on the security incident for progress as the responsible security analyst begins triage.

An integrated risk platform can share information quickly between departments, including a complete audit trail, to comply with stringent requirements such as the GDPR 72-hour breach notification. Built-in workflows speed risk response by automatically generating risks and issues and routing them to the right individuals.

Tech Tip: Different privacy regulations can share many common requirements. Be sure to define a common controls framework so you can test a control once and apply the results to multiple regulations. You can do this either manually or through integration with the **Unified Compliance Framework** from the ServiceNow store.

An integrated risk program for 21st century risk and compliance challenges

It's a relatively safe bet that the scope and potential impact of security threats will continue to increase—and that the compliance burden will continue to grow with them. On top of that, organizations undergoing a digital transformation face new challenges. To counter greater risks and increased pressures, you must embed risk management and compliance activities into new digital workflows and ensure various departments and functional areas think and act as one. They must share information more effectively, identify breaches and disruptions before they wreak significant damage, and utilize cross-functional workflows to enforce the required escalation, review, and response activities. Only an integrated risk program on a common platform can solve this challenge:

- Continuously monitor for risk and compliance across the extended enterprise
- Holistically prioritize risk based on business impact to improve decision making
- Automate repetitive and redundant manual tasks to increase performance

ServiceNow GRC helps make sure you not only comply with new regulations, but thrive in this new era.

Learn more at **www.servicenow.com/grc** and see demos at **DemoNow**

SN-WhitePaper-GRC Use Case Guide-082019